BNL-77063-2006-CP

Development of Human Factors Engineering Guidance for Safety Evaluations of Advanced Reactors

John M. O'Hara – Brookhaven National Laboratory
J. Persensky – Nuclear Regulatory Commission
Autumn Szabo – Nuclear Regulatory Commission

Presented at the

ANS 2006 Winter Meeting & Nuclear Technology Expo

Albuquerque, New Mexico

November 12-16, 2006

Energy Sciences and Technology Department

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

DISCLAIMER

Development of Human Factors Engineering Guidance for Safety Evaluations of Advanced Reactors

John O'Hara
Brookhaven National Laboratory
PO Box 5000
Upton, NY 11973
ohara@bnl.gov

Julius J. Persensky
U.S. Nuclear Regulatory Commission
MS: T10-E50
Washington D.C. 20555-0001

Autumn Szabo
U.S. Nuclear Regulatory Commission
MS: T10-E50
Washington D.C. 20555-0001

Abstract – *Advanced reactors are expected to be based on a concept of operations that is different from what is currently used in today's reactors. Therefore, regulatory staff may need new tools, developed from the best available technical bases, to support licensing evaluations. The areas in which new review guidance may be needed and the efforts underway to address the needs will be discussed. Our preliminary results focus on some of the technical issues to be addressed in three areas for which new guidance may be developed: automation and control, operations under degraded conditions, and new human factors engineering methods and tools.*

I. INTRODUCTION

The U.S. nuclear power community is anticipating the development of advanced reactors (non-light water reactors) envisioned to be ready for deployment in future decades. In addition, the U.S. is participating in international efforts related to the licensing of these advanced designs.

Many of these advanced reactor designs are expected to be based on a concept of operations that is different from today's plants. For example, operators may be expected to concurrently control multiple modules, which could be in different operating states, from a common control room. Operators might be required to monitor online refueling in one module, while other modules are in normal operating states, and another module could be facing a transient. The control rooms are anticipated to be fully computer-based. Procedures are likely to be computerized where control actions could be taken directly from the procedure display, or semi-automated, with the operator authorizing the procedure to take actions. These new concepts of operation will pose new and challenging situations for regulatory reviewers as well as operators and maintainers.

In a report to the U.S. Nuclear Regulatory Commission (NRC), the Brookhaven National Laboratory identified human performance issues associated with advanced reactors which may have to be addressed in future safety reviews (O'Hara, et al. 2004a). These issues were identified by examining current industry developments and making projections into the near and long-term. This was done from four perspectives: reactor design and technology, instrumentation and control technology, human-system integration technology, and human factors engineering (HFE) methods and tools.

The issues identified were organized using a concept of operations framework. This framework is appropriate for plants in the early stages so that design goals and expectations relative to human performance can be identified early in the process. A concept of operations covers all facets of personnel interaction with a complex system; therefore, it provides a good organizational framework with which to cluster and integrate a wide variety of issues. The framework included the following dimensions:

- Role of Personnel and Automation
- Staffing and Training
- Normal Operations Management
- Disturbance and Emergency Management
- Maintenance and Change Management

Two additional dimensions were also included: "Plant Design and Construction" and "HFE Methods and Tools." Thus the issues were organized into seven dimensions in all. The current plan is to prioritize the issues using a Phenomena Identification and Ranking Table (PIRT)-like assessment. Based, in part on that PIRT, future research efforts will be planned.

To ensure minimal human error contribution to the risk associated with the design, construction, operation, testing, and maintenance of these advanced reactor facilities, it is anticipated that new review guidance and tools, developed from the best available technical bases,

may be needed to support licensing and safety monitoring tasks. The NRC Office of Nuclear Regulatory Research has initiated the development of technical bases for three areas: automation and control, operations under degraded conditions, and new HFE methods and tools. This paper summarizes the preliminary results of this effort by focusing on some of the technical issues for which new guidance may need to be developed.

II. HFE INSIGHTS FOR SELECTED HUMAN PERFORMANCE ISSUES

II.A. Automation and Control

Research in other arenas, e.g., transportation, aerospace, military, has shown that a proper mix of human and automatic systems is needed to maximize overall human-system efficiency, reliability, and safety for the selected models of operations. In older plants, the allocation of functions to human and automatic systems was fairly straightforward: they were either automated (i.e., controlled automatically) or manually performed by plant personnel. However, as computers have become more involved in process control, the nature of automation has changed. This paper focuses on three issues: varying levels of automation, automation beyond controls, and use of advanced controls.

Varying Levels of Automation

A significant trend in automation is the increased integration of human and automatic processes in the same control activity. This results in a varying mix of human and automatic actions at different levels of automation. An example is shared control where process sequences are broken up into discrete chunks and the chunks are automated. However, transition from one chunk to the next requires human intervention. The Advanced Boiling Water Reactor plant startup process uses this approach. A similar application is when a control sequence is partially automated and human intervention is needed to provide information not available to the automatic controller. Yet another example is dynamic allocation. In this case, a function can be performed by either automatic systems or by humans. The decision as to who controls the function is made dynamically based on situational considerations, such as the overall workload of personnel.

The evolution of these approaches is in part an effort to minimize the potentially negative effects of automation on human performance (such as loss of situation awareness and complacency). However, the use of differing levels of automation and human action, as well as the methods used to transition between them, may pose a concern and, if so, might need to be evaluated in safety reviews.

Automation beyond Controls

Historically “automation” has meant automating a control function or process. Due to recent technological developments, computer-based systems offer the opportunity to "automate" cognitive activities typically performed as part of the decision-making by plant personnel and to incorporate "intelligence" in the human-system interfaces (HSIs).

In this context, the term "agents" is often used to refer to who or what is performing an activity; i.e., agents are entities that do things. Figure 1 illustrates the generic activities an agent must perform so that functions can be achieved. The agent must monitor the plant to detect conditions indicating that a function has to be performed. The agent must assess the situation and plan a response. Once the response plan is established, it has to be implemented by sending control signals to actuators. The agent must also monitor the function to determine that it is being successfully accomplished and to replan if it is not. Finally the agent must decide when the function has been completed. Human or machine agents can perform any of these activities.

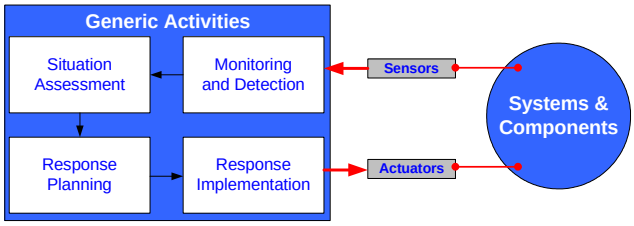

Figure 1: Generic activities performed by agents

An "alarm system," for example, is an automated monitoring and detection system that alerts operators via visual and/or auditory displays when parameters deviate from specified limits or setpoints. However, as more and more functionality is given to HSIs, they evolve toward automatic systems. For example, the only difference between a typical computer-based procedure and an automatic process system is the response implementation. Computer-based procedures (CBPs) can monitor, assess, and plan a response (essentially a paper procedure is a response plan strategy). With most CBPs the operator decides if the action is correct and implements it. If a CBP is also given the means to initiate controls, it becomes an automatic system. Essentially, computerized support systems and intelligent HSIs are semiautomatic systems where human and machine agents are responsible for different generic activities.

The extension of automation beyond simple control functions and the cooperative integration of human and machine resources may need to be addressed in safety reviews.

Use of Advanced Controls

Digital control systems provide the capability to implement much more advanced control algorithms than have been used in plants to date. Current plants rely primarily on single-input, single-output classical control schemes to automate individual control loops. Some multi-variable control schemes have been applied and some plants incorporate a modest level of integration of control loops. However, more advanced control methods and algorithms have not been applied in nuclear plants, although many have been studied in research programs and some have been applied in other industries. It seems likely that advanced reactors will take advantage of more advanced control in order to help meet objectives of increased operability, multi-unit or multi-module control, and reduced staffing.

Advanced control schemes include matrix techniques for optimal control, nonlinear control methods, fuzzy logic, neural networks, adaptive control (a control that modifies its behavior based on plant dynamics), expert systems, state-based control schemes, and schemes that combine multiple control methods in a multi-mode or hierarchical system to achieve optimum performance (see Wood et al., 2003 for a survey of these methods). Application of these advanced techniques will lead to more integrated control of plant systems and processes (versus separate, non-interacting control loops) and greater complexity.

This presents a number of potential issues related to human performance. First, increased control complexity affects design, operations, maintenance, and engineering support personnel. The design and verification and validation of the control schemes will be considerably more difficult to implement than classical control schemes. Once designed and implemented, operations personnel will need sufficient understanding of the control schemes to be able to monitor their performance, determine whether they are working correctly, and be prepared to back them up. Maintenance and engineering support personnel will likewise be affected by the additional complexity and interactivity of the control schemes.

A second issue is related to implementation of intelligent control approaches that learn or change over time. Use of adaptive control methods and techniques, such as on-line knowledge capture and machine learning, offer the advantage that the performance of controls can be improved over time as the plant is operated. However, this also means that the behavior of the controls will be changing. Operation and maintenance personnel will need to be cognizant of these changes and monitor the effects of the changes on plant performance.

Finally, more integrated control schemes can result in greater difficulty for operators when failures occur. This has already been seen in some operating plants that use integrated control systems in which multiple control loops interact when the system is in a fully automatic mode (e.g., the original Babcock & Wilcox Integrated Control System). Failures have the potential to cause multiple control loops to malfunction, placing the operators in a situation in which they must manually control multiple systems. Also, advanced control schemes may have multiple modes of operation and may switch automatically when plant conditions change or failures occur. The operators must maintain an awareness of the current mode of automation, be able to interact effectively with the system during all expected modes, and be prepared to back up the system if required.

A significant safety consideration is how personnel will react to failures of instrumentation and control (I&C) systems when more complex, advanced control schemes, integrated control, multi-mode control, and adaptive control methods are applied. It will be important for plant operators, maintenance personnel, and engineers to be able to distinguish between and react appropriately to: process anomalies, sensor anomalies or failures, control adjustments or adaptations made automatically by the system, and control system failures

II.B. Operations under Degraded Conditions

Advanced reactors are expected to rely heavily on integrated digital I&C equipment for Reactor Protection Systems and Engineered Safety Feature Actuation System. The I&C systems of a nuclear power plant have three major roles. First, they are the ‘eyes and ears’ of the operator. If properly planned, designed, constructed and maintained, they will provide accurate and appropriate information and permit judicious action during both normal and abnormal operation. They are, therefore, with the human operator, vital to the safe and efficient operation of the plant. Second, under normal operating conditions they provide automatic control, both of the main plant and of many ancillary systems. This allows the operator time to observe plant behavior and monitor what is happening so that the right corrective action can be taken quickly, if required. Third, under abnormal conditions, they provide rapid automatic action to protect both the plant and the environment.

Even though digital systems are typically highly reliable, their potential failure or degradation could significantly impact plant response and plant safety. While digital technology has the capability to improve operational performance, there are challenges to the introduction of this technology into nuclear power plants. These challenges include: (1) rapid changes in digital technology could impact digital system design, testing and application; (2) the increased complexity of digital technology, compared to its analog counterpart, could potentially require enhanced licensing reviews, complicate configuration control, and require detailed documentation; and (3) the impact of unique failure modes and degradations associated with digital technology on plant response, including the required operator actions, may be challenging.

Thus it is important to identify the degradation and failure modes of digital I&C systems during abnormal and accident conditions that could impact on operations and crew monitoring and control functions.

I&C degradation may be caused by a variety of events, such as instrument failure, computer failures, seismic events, fire and smoke damage, internal flooding, and loss of electrical power. These events may cause a range of failures from individual control room instruments to more significant degradations, such as the loss of all displays. Issues associated with this topic include:

- *Detection of Digital System Failure* - The loss of hardwired displays and controls is readily apparent to plant personnel. However, the degradation modes and failures in digital systems can be more difficult to detect, especially in the case of degradations short of complete failure. The reason for this is that much of the information with which the crew interacts will be at a high level as compared to the single sensor-single display relationship that characterizes more traditional equipment. Information displays, for example, will often represent the integration of many lower level data points. The impact of sensor and processing degradation on these higher-level displays is not well understood. In addition, such features as improved system diagnostics and signal validation will have an effect on the operator's ability to monitor, detect, and control system failures.

- *Transition to Back-up Systems* - Upon failures of digital systems, crews may have to transition to use of the hardwired controls and displays and paper procedures where available. Crew interactions with these technologies are very different from their interaction when using digital systems. Digital systems provide a great deal of support to crews in terms of information access and suitability to ongoing task requirements that is not available from conventional, analog-based technology. The crews can become dependent on this support, so crews will need multiple competencies to respond to these incidents.

- *Teamwork* - Prior NRC-sponsored research has shown that digital systems have a significant impact on crew teamwork and coordination (Roth & O'Hara, 2002). This was an unanticipated consequence in many of the first plant modernization programs that occurred in foreign plants. For example, the availability of improved monitoring, decision support, controls, and automation, frequently alters the crew's role more toward system supervisors. This is because the digital systems perform many of the lower level activities associated with data gathering and processing. Thus, the crews are freed from these lower level activities. This has often resulted in a shift to less teamwork, less communication, and more difficultly for crew members to monitor each other's activities. With respect to the latter, when crew members are located at individual panels, it is relatively easy to see what they are doing. By contrast, when crew members are seated in front of computer monitors, it is much more difficult to be aware of what they are doing. When the digital systems are lost, the crew must shift its activities to once again accomplish the lower-level responsibilities that the digital system performed. In this case, the type of teamwork needed is more similar to present day control rooms.

All of these issues may become more significant as new generations of operators, trained mainly on digital system operations, have to cope with abnormal situations. Current crews are already well trained in the use of conventional equipment and in the teamwork requirements associated with its use. Succeeding generations of operators will become less and less familiar with the conventional equipment. New approaches to the review of operations under degraded conditions may be needed to ensure effective and safe management of these situations.

II.C. New HFE Methods and Tools

HFE methods are used to analyze, design, test and evaluate the HFE aspects of a plant, such as the HSI. The methods are important because NRC HFE reviews are design process oriented (NUREG-0711, 2004), thus, the criteria are mostly technology neutral with regard to reactor design. However, the HFE review criteria are not neutral with respect to the HFE methods that are used as part of the design process. This will be important for advanced reactor reviews because the diversity of reactor types, HSIs, and operational concepts will increase, especially for advanced reactors.

Trends and issues in emerging HFE methods were identified in the nuclear industry, related industries, and the military arena through a review of the literature and discussions with subject matter experts. Well over 100 new methods and tools were identified. The methods were then organized into the following categories: Analysis, Design, and Test and Evaluation.

Analysis methods are used to develop detailed, system-specific information and requirements for inputs to HFE design activities. While there is general agreement on the importance of beginning HFE activities early in the design process, there is a need for more formal and structured approaches. Areas where guidance is needed include: operating experience analysis and the development of lessons learned, function allocation, human reliability analysis (HRA), and the development and application of knowledge engineering techniques. Two examples are given below.

Because they primarily focus on conventional manual actions, current HRA methods may not be well suited to advanced designs which incorporate increased automation, alternative concepts of operations, and intelligent agents. HRA will be further constrained by the lack of data to support human error probability estimates. Information to address this gap may be needed.

On the other hand, one area that has been evolving rapidly is task analysis. Recent advances in work analysis, cognitive task analysis, and cognitive engineering are especially applicable to supervisory control tasks. However, there is a lack of information on the appropriate application and selection of such methods. The review of appropriate analysis methods may need to be improved.

Design methods translate requirements into detailed designs. Advanced methods are evolving to develop designs in far less time and with more user input. Using techniques such as rapid prototyping, designs quickly evolve through a number of iterations with users to obtain feedback and make HSI modifications. The cycle is repeated until the design is completed. A potential concern relates to the technical basis on which these HSIs are developed, since the design may be based on a limited sample of users and may not incorporate tested and validated design features. Without information on the use of such techniques the resulting design may not be technically sound.

Future HSIs are also likely to provide information at much higher levels than exist in today's plants, such that base data are integrated or aggregated and the operator may not have access to the base data. Lower-level information will be integrated and processed to provide more meaningful information to operators regarding plant status. While this type of information display may be a promising advance, there are no well-defined processes for conducting the analyses needed to specify them or to review the process at the design stage.

A key issue regarding test and evaluation methods is how the effects of advanced and intelligent systems can be evaluated. Evaluations are becoming more performance-based, thus performance measurement and criteria are important considerations. Measures that reflect integrated system performance may be necessary for which criteria for system acceptability can be established. Further, since personnel work as teams, modeling and measurement of effective team performance is an important consideration.

In a performance-based approach, validation of integrated systems is a key activity and many aspects of its methodology are being impacted by technology. For example, one significant component is the testbed, such as a full-mission simulator. New technologies are being developed that provide alternatives to traditional testbeds, e.g., virtual reality (VR). An important question that should be addressed is the validation of VR models and the understanding of how the methodology is applied. In general, clearly defined and accepted methodological criteria are needed to review licensee submittals which are based on the use of VR techniques.

While the above issues relate to measuring actual personnel performance, current trends are to obtain "performance data" from human performance models, such as task network models and discrete event simulation. Since operator availability is limited and the means to collect data can be resource intensive, models are an attractive alternative to extensive man in the loop simulator testing. As modeling improves, its application will be extended to more complex design and evaluation situations. Both the validity of the modeling and its results needs to be considered in a licensing process.

When looking across the new methods and tools, several major trends were identified.

- Computer-based aids are being used for performing traditional analyses, such as link analysis.
- Rapid development tools/approaches, such as rapid prototyping, can be used to develop interfaces more rapidly, at less cost, through the use of iterative methods, incorporating user input and feedback
- Computer-based design tools (e.g. rapid prototyping), that are not tied to design guidelines, are used in iterative design processes.
- HFE methods are being integrated to address multiple aspects of the design process.

• Intelligent advisors are being used in computer-aided design.

• Human performance models are being used as a supplement to or replacement for data collection based on actual users).

• Techniques such as virtual reality are being used to support design and evaluation as a supplement to or replacement of physical mockups and simulators.

• There is more focus on methods that address human cognition, such as cognitive task analysis and knowledge engineering.

• Design is being extended into operations using flexible and modifiable HSIs to provide users with tools that allow them to change HSIs to suit their needs.

HFE methods are rapidly evolving and generating new approaches to designing the HFE aspects of plants. Thus, improvements to the methods and criteria used for reviews may be needed to keep pace with the advances in analysis, design, test and evaluation methodologies.

III. DISCUSSION

Advanced plants will offer the potential for improvements in performance and safety. However, there are still challenges ahead, especially as personnel and technology are integrated into final designs. While these advances may pose challenges for vendors and licensees, they will potentially present challenges to reviewers as well. Research to develop the technical basis from which regulatory review guidance could be developed to meet these challenges has been initiated. The intent of these efforts is to set clear expectations for how advanced designs could be evaluated, to reduce regulatory uncertainty, and to provide a well-defined path to licensing of advanced reactors.

ACKNOWLEDGMENTS

This paper is based on research that is sponsored by the U. S. Nuclear Regulatory Commission. The views presented in this paper represent those of the authors alone and not necessarily those of the NRC.

REFERENCES

[1] O'HARA, J., HIGGINS, J., BROWN, W. & FINK, R., "Human Performance Issues In Advanced Reactors" (Report No: Y6646-T4-11/03), Upton, NY: Brookhaven National Laboratory (2004a).

[2] O'HARA, J., HIGGINS, J., PERSENSKY, J., LEWIS, P., & BONGARRA, J., "Human Factors Engineering Program Review Model" (NUREG-0711, Rev. 2), Washington, D.C.: U.S. Nuclear Regulatory Commission (2004b).

[3] ROTH, E. & O'HARA, J., "Integrating Digital and Conventional Human System Interface Technology: Lessons Learned From A Control Room Modernization Program" (NUREG/CR-6749), Washington, D.C.: U.S. Nuclear Regulatory Commission (2002).

[4] WOOD, R., ANTONESCU, C., ARNDT, S., BRITTON, C., BROWN-VANHOOZER, S. CALVERT, J. DAMIANO, B., EASTER, J., FREER, M. , MULLENS, J., NEAL, J., PROTOPOPESCU,V., SHAFFER, R., SCHRYVER, J., SMITH, C. TUCKER, R., UHRIG, R., UPADHYAYA, B., WETHERINGTON, G., WILSON, T., WHITE, J., & WHITUS, B., "Emerging Technologies in Instrumentation and Controls" (NUREG/CR-6812), Washington, D.C.: U.S. Nuclear Regulatory Commission (2003).